IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

PATRICK REYNOLDS and **DANIEL LEWIS** on behalf of themselves and all others similarly situated, Plaintiffs, v. **MARYMOUNT MANHATTAN COLLEGE,** Defendant.	Case No. Judge **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Patrick Reynolds and Daniel Lewis ("Plaintiffs") bring this Class Action Complaint against Marymount Manhattan College ("MMC" or "Defendant"), as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendant MMC, a private college located in New York City, New York, to seek damages for themselves and other similarly situated current and former students, admission applicants, or any other person(s) impacted in the data breach at issue ("Class Members") who they seek to represent, as well as other equitable relief, including, without limitation, injunctive relief designed to protect the very sensitive information of Plaintiffs and other Class Members. This action arises from Defendant's failure to properly secure and safeguard personally identifiable information, including without limitation, unencrypted and unredacted names, Social Security numbers, student IDs, dates of birth, Social Security numbers,

employee IDs, "as well as some other types of information," including payment and credit card information[1] (collectively, "personally identifiable information" or "PII").

2. Plaintiffs allege MMC failed to provide timely, accurate and adequate notice to Plaintiffs and Class Members who were or are past and current students, employees, parents, and applicants to MMC. Plaintiffs' and Class Members' knowledge about what personal identifiable information MMC lost, as well as precisely what types of information was unencrypted and in the possession of unknown third parties, was unreasonably delayed by MMC's nearly nine-month delay in warning impacted persons after it first learned of the data breach.

3. On or about August 3, 2022, MMC finally notified state Attorneys General and many Class Members about a widespread data breach in which the sensitive PII of individuals was accessed and acquired by a malicious actor. MMC explained in its required notice letter that it discovered *on November 12, 2021* (almost nine months earlier) that it "experienced a network disruption" and that files on its network were accessed and acquired by the unknown actor (the "Data Breach").[2]

4. In November 2021, MMC chose not to notify affected individuals or, upon information and belief, anyone of its data breach instead choosing to address the incident in-house by implementing unknown safeguards to some aspects of its computer security. It then, without warning persons impacted by the Data Breach, simply resumed its normal business operations.

5. Over eight months later, on July 28, 2022, MMC concluded its investigation and determined that Class Members' PII had been impacted and taken from its network.[3]

---

[1] https://www.mmm.edu/offices/information-technology/cybersecurity/
[2] Office of the Vermont Attorney General, https://ago.vermont.gov/blog/2022/08/03/marymount-manhattan-college-data-breach-notice-to-consumers/ (last visited August 9, 2022) (hereafter "Notice Letter").
[3] *Id.*

6. MMC still took nearly a week to notify state Attorneys General and Students about the widespread data breach.[4]

7. According the Notice Letter it sent Attorneys General and some Class Members, MMC "secure[d] the network environment" hired "cybersecurity experts" to investigate the breach of MMC's systems, and determined that Plaintiffs' and Class Members' personal identifiable information (including but not limited to full names and Social Security numbers) was present and potentially stolen by the unauthorized person at the time of the incident.[5]

8. MMC's Notice Letter plainly admits that Plaintiffs and Class Members' PII were compromised when the "unknown actor gained access to and obtained data from the MMC network without authorization." This means that Plaintiffs and Class Members' PII was exfiltrated by the unauthorized actors during the Data Breach.

9. Plaintiffs and the Class Members in this action were, according to MMC, "past and current students, employees, parents, and applicants to MMC."[6] The first that Plaintiffs and the Class Members learned of the November 2021 Data Breach was when they received by U.S. Mail Notice of Data Breach letters dated August 3, 2022, directly from MMC.

10. In its Notice Letters, sent to state and federal agencies and some Class Members, MMC failed to explain why it took the company nearly nine months (from November 12, 2021, when MMC detected unusual activity to August 3, 2022) to alert Class Members that their sensitive PII had been exposed.[7] As a result of this delayed response, Plaintiffs and Class Members were unaware that their PII had been compromised, and that they were, and continue to be, at significant risk to identity theft and various other forms of personal, social, and financial harm.

---

[4] *Id.*
[5] *Id.*
[6] https://www.mmm.edu/offices/information-technology/cybersecurity/
[7] Notice Letter

11. Further, MMC's letters noticing Plaintiff Reynolds and certain Class Members do not explain the precise scope of the Data Breach or how long the unauthorized actor had access to Defendant's network.[8] In fact, the letter Plaintiff Reynolds received is markedly different from that Defendant provided to the Attorneys General offices. Plaintiff Reynold's letter simply states:

> Marymount Manhattan College ("MMC") is writing to inform you about an information security incident that involved your personal information. We are writing to inform you of the incident and to advise you of certain steps that you can take to help protect your personal information.

12. The letter provides no further information regarding the Data Breach and only goes on to recommend how to place a security freeze on a credit report and how to sign up for identity monitoring services offered by Defendant in response to the Data Breach. The letter Plaintiff Reynolds received does not explain when or how the Data Breach occurred, when MMC detected the Data Breach, what steps MMC took following the Data Breach, or most importantly, which of Plaintiffs' personal information was impacted by the Data Breach. It is wholly different from the Notice Letters sent to state Attorneys General.

13. Plaintiffs' and Class Members' unencrypted, unredacted PII was compromised due to MMC's negligent and/or careless acts and omissions, and due to the utter failure to protect Class Members' sensitive data. Hackers obtained their PII because of its value in exploiting and stealing the identities of Plaintiffs and similarly situated Class Members. The risks to these persons will remain for their respective lifetimes.

14. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of MMC's failure to: (i) adequately protect Plaintiffs' and Class Members' PII; (ii) warn Plaintiffs and Class Members of its inadequate information security practices; and (iii) effectively monitor MMC's network for security vulnerabilities and incidents. MMC's conduct amounts to

[8] *Id.*

negligence and violates federal and state statutes.

15. Plaintiffs and Class Members have suffered injury as a result of MMC's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; change their usernames and passwords on their accounts; investigate, correct and resolve unauthorized debits; deal with spam messages and e-mails received subsequent to the Data Breach, (v) charges and fees associated with fraudulent charges on their accounts, and (vi) the continued and certainly an increased risk to their PII, which remains in MMC's possession and is subject to further unauthorized disclosures so long as MMC fails to undertake appropriate and adequate measures to protect the PII. These risks will remain for the lifetimes of Plaintiffs and Class Members.

16. MMC disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or at the very least negligently failing to take and implement adequate and reasonable measures to ensure that its Students' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

Plaintiff Patrick Reynolds

17. Plaintiff Patrick Reynolds is a resident and citizen of Massachusetts, residing in Hudson, Massachusetts. Mr. Reynolds received a Notice of Data Security Incident letter from MMC, dated August 3, 2022 by U.S. Mail.

Plaintiff Daniel Lewis

18. Plaintiff Daniel Lewis is a resident and citizen of Connecticut, residing in Westport, Connecticut. Mr. Lewis received a Notice of Data Security Incident letter from MMC, dated August 3, 2022 by U.S. Mail.

Defendant Marymount Manhattan College

19. Defendant MMC is a private college located in New York City, New York, which has a principal place of business at 221 East 71st Street, New York, New York 10021.

20. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

21. All of Plaintiffs' claims stated herein are asserted against MMC and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

22. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Plaintiffs (and many members of the Class) and Defendant are citizens of different states. Plaintiff Reynolds is a citizen

of Massachusetts and Plaintiff Lewis is a citizen of Connecticut. Defendant is a New York institution with its principal place of business is located at 221 East 71st Street, New York, New York 10021.

23. This Court has general personal jurisdiction over Defendant because Defendant's principal place of business is in New York City, New York and Defendant regularly conducts business in New York.

24. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District, and Defendant conducts substantial business in this District.

IV. FACTUAL ALLEGATIONS

Background

25. MMC is a private college located in New York City, New York, which has a principal place of business at 221 East 71st Street, New York, New York 10021.

26. In its Notice Letters sent to Attorneys General, MMC claims that it "takes the privacy and security of the personal information in our possession very seriously."

27. On its own website, MMC holds itself out as committed to protecting the privacy of its students. MMC states it "does not sell, rent, give away or loan any identifiable information to any third party other than agents and contractors of MMC."[9]

28. As MMC acknowledges in its Notice Letters, protection of personally identifiable information is something it takes "very seriously."

29. Plaintiffs and the Class Members, as current or former students, applicants, parents of the same, or employees of MMC, reasonably relied (directly or indirectly) on this sophisticated

[9] *See* https://www.mmm.edu/offices/information-technology/mmc-privacy-statement/ (last accessed August 9, 2022).

higher education institution to keep their sensitive PII confidential; to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their PII. People demand security to safeguard their PII, especially when Social Security numbers and other sensitive PII is involved as here.

30. MMC had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII from involuntary disclosure to third parties and as evidenced by the Data Breach, it failed to adhere to that duty.

The Data Breach

31. In early August 2022, MMC first began notifying Class Members and state Attorneys General ("AGs") about a widespread breach of its computer systems and involving the sensitive personal identifiable information of "past and current students, employees, parents, and applicants to MMC."[10] MMC explained that the Data Breach was detected in November 2021.[11]

32. According to its Notice Letters, MMC explained it discovered *on November 12, 2021* (nearly nine months earlier) that it "experienced a network disruption." MMC discovered that files on its network were accessed and acquired by the unknown actor.

33. On or about August 3, 2022, MMC notified state Attorneys General and many impacted persons about a widespread data breach involving sensitive PII of thousands of individuals.

34. In November 2021, MMC chose not to notify affected individuals or, upon information and belief, anyone, of its data breach instead choosing to address the incident in-house by implementing unknown safeguards to some aspects of its computer security. It then simply

[10] Office of the Vermont Attorney General, *https://ago.vermont.gov/blog/2022/08/03/marymount-manhattan-college-data-breach-notice-to-consumers/* (last accessed August 9, 2022); https://www.mmm.edu/offices/information-technology/cybersecurity/.
[11] *Id.*

resumed its normal business operations.

35. Over eight months later, on July 28, 2022, MMC concluded its investigation and admitted that Plaintiffs' and Class Members' PII had been impacted and taken from its network.[12]

36. MMC hired "cybersecurity experts" and "secure[d] the network environment" of MMC's systems and determined that Plaintiffs' and Class Members' PII (including but not limited to full names and Social Security numbers) was present and potentially stolen by the unauthorized person at the time of the incident. [13]

37. Plaintiffs and Class Members in this action were, according to MMC, current, former and prospective students at MMC, their parents, and MMC employees. The first that Plaintiffs and Class Members learned of the Data Breach was nearly nine months after MMC learned of the Data Breach. Plaintiffs and Class Members still have not learned the full scope of the Data Breach or precisely what information was impacted. MMC's letters to Plaintiff Reynolds simply states there was, "an information security incident that involved your personal information. We are writing to inform you of the incident and to advise you of certain steps that you can take to help protect your personal information." The letter offers Plaintiff Reynolds no further details about the personal information at issue.

38. According to MMC's website, the confidential information that was accessed without authorization included at least names, Social Security numbers, student IDs, date of birth, social security numbers, employee IDs, "as well as some other types of information," including payment and credit card information.

39. Upon information and belief, the PII was not encrypted prior to the data breach.

[12] *Id.*
[13] *Id.*

40. Upon information and belief, the cyberattack was targeted at MMC as a higher education institution that collects and maintains valuable personal, health, tax, and financial data.

41. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the PII of Plaintiffs and the Class Members.

42. MMC admitted in its Notice Letter to the Attorneys General that their systems were subjected to unauthorized access in November 2021. In the Notice Letters, MMC made no indication to either group (AGs or Class) that the exfiltrated PII was retrieved from the cybercriminals who took it, nor how long the data was available to these unauthorized actors.[14]

43. With its offer of credit and identity monitoring services to victims, MMC is acknowledging that the impacted persons are subject to an imminent threat of identity theft and financial fraud as a result of its failure to protect the PII it collected and maintained.

44. In response to the Data Breach, MMC claims that "additional security features were also implemented to reduce the risk of a similar incident occurring in the future."[15] MMC admits additional security was required, but there is no indication what these measures entail and whether these steps are adequate to protect Plaintiffs' and Class Members' PII going forward.

45. MMC had obligations created by contract, industry standards, common law, and representations made to its Plaintiffs and Class Members to keep the PII that was entrusted to MMC confidential, and to protect the PII from unauthorized access and disclosure.

46. Plaintiffs and Class Members provided their PII to MMC with the reasonable expectation that MMC as a higher education institution would comply with its duty and obligations and representations to keep such information confidential and secure from unauthorized access.

[14] *See* Notice Letter
[15] *Id*.

47. MMC failed to uphold its data security obligations to Plaintiffs and Class Members. As a result, Plaintiffs and Class Members are significantly harmed and will be at a high risk of identity theft and financial fraud for many years to come.

48. MMC did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining, causing Plaintiffs' and Class Members' PII to be exposed.

Securing PII and Preventing Breaches

49. MMC could have prevented this Data Breach by properly encrypting or otherwise protecting their equipment and computer files containing PII.

50. In its notice letters, MMC acknowledged the sensitive and confidential nature of the PII. To be sure, collection, maintaining, and protecting PII is vital to virtually all of MMC's business purposes as a private higher education institution. MMC acknowledged through its conduct and statements that the misuse or inadvertent disclosure of PII can pose major privacy and financial risks to impacted individuals, and that under state law they may not disclose and must take reasonable steps to protect PII from improper release or disclosure.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice

51. It is well known that PII, including Social Security numbers and financial account information in particular, is an invaluable commodity and a frequent target of hackers.

52. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[16]

53. Of the 1,473 recorded data breaches, 108 of them were in the banking/credit/financial industry, with the number of sensitive records being exposed exceeding

[16] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed December 10, 2021)

100 million. In fact, over 62% of the 164 million sensitive records exposed in data breaches in 2019 were exposed in those 108 breaches in the banking/credit/financial sector.[17]

54. The 108 reported financial sector data breaches reported in 2019 exposed 100,621,770 sensitive records, compared to 2018 in which only 1,778,658 sensitive records were exposed in financial sector breaches.[18]

55. Individuals place a high value not only on their PII, but also on the privacy of that data. For the individual, identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

56. Individuals are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as your DNA to hackers." There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their Social Security numbers have been accessed, Plaintiffs and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems … and won't guarantee … a fresh start."

57. In light of recent high profile data breaches, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), MMC knew or should have known that its electronic records would be targeted by cybercriminals.

[17] *Id*.
[18] *Id* at p. 15.

58. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

59. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite their own acknowledgment of its duties to keep PII private and secure, MMC failed to take appropriate steps to protect the PII of Plaintiffs and the proposed Class from being compromised.

At All Relevant Times MMC Had a Duty to Plaintiffs and Class Members to Properly Secure their Private Information

60. At all relevant times, MMC had a duty to Plaintiffs and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiffs and Class Members, and to *promptly* notify Plaintiffs and Class Members when MMC became aware that their PII may have been compromised.

61. MMC's duty to use reasonable security measures arose as a result of the special relationship that existed between MMC, on the one hand, and Plaintiffs and the Class Members, on the other hand. The special relationship arose because Plaintiffs and the Members of the Class entrusted MMC with their PII as a condition of receiving educational services for themselves or their children or when they applied for or accepted employment at MMC.

62. MMC had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, MMC breached its common law, statutory, and other duties owed to Plaintiffs and Class Members.

63. Security standards commonly accepted among businesses that store PII using the

internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

64. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[19] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[20]

65. The ramifications of MMC's failure to keep Plaintiffs' and Class Members' PII secure are long lasting and severe. Once PII is stolen, particularly Social Security numbers as here, fraudulent use of that information and damage to victims is likely to continue for years.

[19] 17 C.F.R. § 248.201 (2013).
[20] *Id*.

The Value of Personal Identifiable Information

66. PII of data breach victims remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[21] According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[22]

67. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls

[21] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed December 10, 2021).

[22] *Dark Web Price Index 2021*, Zachary Ignoffo, March 8, 2021, *available at*: https://www.privacyaffairs.com/dark-web-price-index-2021/ (last accessed December 10, 2021).

> from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[23]

68. Furthermore, trying to change or cancel a stolen Social Security number is no minor task. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

69. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[24]

70. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[25]

71. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their

---

[23] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed December 10, 2021).

[24] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed December 10, 2021).

[25] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed December 10, 2021).

birthdate, birthplace, and mother's maiden name.[26]

72. Given the nature of MMC's Data Breach, as well as the long delay in notification to Class Members, it is foreseeable that the compromised PII has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiffs' and Class Members' PII can easily obtain Plaintiffs' and Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

73. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.[27] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

74. To date, MMC has offered Plaintiffs and Class Members *only one or two years* of identity monitoring services despite the almost nine-month delay from their discovery of the Data Breach to the Notice Letters. The offered services are inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

75. The injuries to Plaintiffs and Class Members were directly and proximately caused by MMC's failure to implement or maintain adequate data security measures to protect PII that it maintained.

---

[26] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.

[27] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes, Mar 25, 2020, *available at*: https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last accessed December 10, 2021).

MMC Failed to Comply with FTC Guidelines

76. Federal and State governments have established security standards and issued recommendations to lessen the risk of data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[28]

77. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[29] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

78. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[30]

79. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

---

[28] Federal Trade Commission, *Start With Security, available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed December 10, 2021).

[29] Federal Trade Commission, *Protecting Personal Information: A Guide for Business, available at*: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last accessed December 10, 2021).

[30] FTC, *Start with Security*, *supra* note 34.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

80. The FTC has brought enforcement actions against businesses for failing to protect consumer and consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

81. Because Class Members entrusted MMC with their PII directly or indirectly through MMC, MMC had, and has, a duty to the Class Members to keep their PII secure.

82. Plaintiffs and the other Class Members reasonably expected that when they provide PII to their college, that MMC would safeguard their PII.

83. MMC was at all times fully aware of its obligation to protect the personal data of Students, including Plaintiffs and members of the Classes. MMC was also aware of the significant repercussions if it failed to do so.

84. MMC's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—including Plaintiff's and Class Members' full names, Social Security numbers, and other highly sensitive and confidential information—

constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Plaintiffs and Class Members Have Suffered Concrete Injury As A Result Of Defendant's Inadequate Security And The Data Breach It Allowed.

85. Plaintiffs and Class Members reasonably expected that Defendant would provide adequate security protections for their PII, and Class Members provided Defendant with sensitive personal information, including their Social Security numbers.

86. Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay Defendant for their education, Plaintiffs and other Class Members reasonably understood and expected that their PII would be protected with data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected. As such, Plaintiffs and the Class Members suffered pecuniary injury.

87. Cybercriminals capture PII to exploit it; the Class Members are now, and for the rest of their lives will be, at a heightened risk of identity theft. Plaintiffs have also incurred (and will continue to incur) damages in the form of, *inter alia*, loss of privacy and costs of engaging adequate credit monitoring and identity theft protection services.

88. The cybercriminals who obtained the Class Members' PII may exploit the information they obtained by selling the data in so-called "dark markets." Having obtained these names, addresses, Social Security numbers, and other PII, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

- obtaining employment;
- obtaining a loan;
- applying for credit cards or spending money;

- filing false tax returns;
- stealing Social Security and other government benefits; and
- applying for a driver's license, birth certificate, or other public document.

89. In addition, if a Class Member's Social Security number is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

90. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiffs and the other Class Members have been deprived of the value of their PII, for which there is a well-established national and international market.

91. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.[31]

92. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiffs and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.[32] Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach."[33] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places

[31] *Id.*
[32] *Data Breach Victims More Likely To Suffer Identity Fraud*, INSURANCE INFORMATION INSTITUTE BLOG (February 23, 2012), http://www.iii.org/insuranceindustryblog/?p=267 (last accessed December 10, 2021).
[33] Susan Ladika, *Study: Data Breaches Pose A Greater Risk*, CREDITCARDS.COM (July 23, 2014), http://www.creditcards.com/credit-card-news/data-breach-id-theft-risk-increase-study-1282.php (last accessed December 10, 2021).

consumers at a substantial risk of fraud."[34] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' PII will do so at a later date or re-sell it.

93. As a result of the Data Breach, Plaintiffs and Class Members have already suffered damages.

94. In its Notice Letter, Defendant represented to the AGs that it initially discovered the Data Breach on November 12, 2021, and admitted files were accessed and acquired by the cybercriminals.

95. In this case, according to Defendant's notification to the state Attorneys General, cybercriminals had access to and acquired Class Members' data at least on November 12, 2021, yet its notice letters about that Data Breach did not go out until August 3, 2022. This is tantamount to the cybercriminals having over eight-months of a head start on stealing the identities of Plaintiffs and Class Members.

Plaintiff Reynolds's Experience

96. On or about August 3, 2022, Mr. Patrick Reynolds, a citizen and resident of Hudson, Massachusetts, received a Notice of Data Security Incident Letter by US. Mail. The letter Plaintiff received lacked any detail about the scope of the Data Breach, which of his PII was involved, when the Data Breach was detected, or what steps, if any, that Defendant took in response to the Data Breach. The letter Plaintiff Reynolds received was markedly different from the Notice Letter sent to the Attorneys General.

---

[34] THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH- IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS, (*available at* https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf) (last accessed December 10, 2021).

97. When applying for admission and while a student at MMC, Plaintiff Reynolds provided his PII to MMC in order to gain admission, financial aid, receive his education, and under state and federal law, he was required to do so. He reasonably relied on MMC, a higher education institution, to protect the security of his PII.

98. As a result of the Data Breach and the information that he received in the letter, Mr. Reynolds has spent many hours dealing with the consequences of the Data Breach (considering closing and opening bank accounts, changing banks, changing passwords, and now self-monitoring his bank and credit accounts), as well as his time spent verifying the legitimacy of the Notice Letter, communicating with MMC representatives, communicating with his bank, and exploring credit monitoring and identity theft insurance options. This time has been lost forever and cannot be recaptured and time that he could have spent on other pursuits like work or leisure activities.

99. Mr. Reynolds is very careful about sharing his own personal identifying information and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

100. Mr. Reynolds stores any and all documents containing PII in a secure location, and destroys any documents he receives in the mail that contain any PII or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

101. Mr. Reynolds suffered actual injury and damages due to MMC's mismanagement of his PII before the Data Breach.

102. Mr. Reynolds suffered actual injury in the form of damages and diminution in the value of his PII—a form of intangible property that he entrusted to MMC, which was compromised

in and as a result of the Data Breach.

103. Mr. Reynolds suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and he has suffered extreme anxiety and increased concerns for the theft of his privacy since he received the Notice Letter. He is especially concerned about the theft of his full name paired with his Social Security number.

104. Mr. Reynolds has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII, especially his Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

105. Mr. Reynolds has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in MMC's possession, is protected and safeguarded from future breaches.

Plaintiff Lewis's Experience

106. On or about August 3, 2022, Mr. Daniel Lewis, a citizen and resident of Westport, Connecticut, received a Notice of Data Security Incident Letter by US. Mail. The letter Mr. Lewis received was substantially similar to those provided to the AG's but still lacked any detail about the scope of the Data Breach, the means of attack, or what specific steps that Defendant took in response to the Data Breach. The letter did disclose that Mr. Lewis's name and Social Security number were accessed and acquired in the Data Breach.

107. When applying for admission and while a student at MMC, Mr. Lewis provided his PII to MMC in order to gain admission, financial aid, receive his education, and under state and federal law, he was required to do so. He reasonably relied on MMC, a higher education institution, to protect the security of his PII.

108. As a result of the Data Breach and the information that he received in the letter, Mr. Lewis has spent many hours dealing with the consequences of the Data Breach (considering closing and opening bank accounts, changing banks, changing passwords, and now self-monitoring his bank and credit accounts), as well as his time spent verifying the legitimacy of the Notice Letter, communicating with MMC representatives, communicating with his bank, and exploring credit monitoring and identity theft insurance options. This time has been lost forever and cannot be recaptured and time that he could have spent on other pursuits like work or leisure activities.

109. Mr. Lewis is very careful about sharing his own personal identifying information and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

110. Mr. Lewis stores any and all documents containing PII in a secure location, and destroys any documents he receives in the mail that contain any PII or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

111. Mr. Lewis suffered actual injury and damages due to MMC's mismanagement of his PII before the Data Breach.

112. Mr. Lewis suffered actual injury in the form of damages and diminution in the value of his PII—a form of intangible property that he entrusted to MMC, which was compromised in and as a result of the Data Breach.

113. Mr. Lewis suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and he has suffered extreme anxiety and increased concerns for the theft of his privacy since he received the Notice Letter. He is especially concerned about the theft of his full

name paired with his Social Security number.

114. Mr. Lewis has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII, especially his Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

115. Mr. Lewis has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in MMC's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

116. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated.

117. The Class that Plaintiffs seek to represent is defined as follows:

> All persons residing in the United States whose PII was compromised in the data breach announced by MMC in August 2022. (the "Class").

118. Excluded from the Class are the following individuals and/or entities: MMC, and MMC's parents, subsidiaries, affiliates, officers and directors, and any entity in which MMC has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

119. Plaintiffs reserve the right to modify or amend the definition of the proposed class and any future subclass before the Court determines whether certification is appropriate.

120. Numerosity. The Members of the Class are so numerous that joinder of all of them

is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of thousands of individuals whose sensitive data was compromised in Data Breach.

121. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PII;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their PII;

f. Whether Defendant breached its duty to Class Members to safeguard their PII;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breach implied contracts with Plaintiffs and Class Members;

l. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

n. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

122. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

123. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

124. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

125. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high

and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

126. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

127. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because MMC would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

128. The litigation of the claims brought herein is manageable. MMC's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

129. Adequate notice can be given to Class Members directly using information maintained in MMC's records.

130. Unless a Class-wide injunction is issued, MMC may continue in its failure to properly secure the PII of Class Members, MMC may continue to refuse to provide proper notification to Class Members regarding the Data Breach, the PII MMC continues to maintain will remain at risk of future breach, and MMC may continue to act unlawfully as set forth in this Complaint.

131. Further, MMC has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive relief with regard to the Class Members as a whole is appropriate.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

132. Plaintiffs restate and reallege all of the foregoing paragraphs as if fully set forth herein.

133. As a condition of applying for enrollment, gaining financial aid, or remaining a student at MMC, prospective, current, and former students and/or their parents are obligated to provide MMC with certain PII, including but not limited to, their names, Social Security numbers, student IDs, date of birth, social security numbers, employee IDs, "as well as some other types of information," including payment and credit card information.

134. Plaintiffs and Class Members entrusted their PII to MMC on the premise and with the understanding that MMC would safeguard their information, use their PII for legitimate business purposes only, and/or not disclose their PII to unauthorized third parties.

135. MMC has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

136. MMC knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII involved an unreasonable risk of harm to Plaintiffs and Class Members, even if the harm occurred through the criminal acts of a third party.

137. MMC had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing MMC's security protocols to ensure that Plaintiffs' and Class Members' information in MMC's possession was adequately secured and protected.

138. MMC also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiffs' and Class Members' PII.

139. A breach of security, unauthorized access, and resulting injury to Plaintiffs and Class Members was reasonably foreseeable, particularly in light of MMC's business as higher education institution, for which the diligent protection of PII is a continuous forefront issue.

140. Plaintiffs and Class Members were the foreseeable and probable victims of MMC's inadequate security practices and procedures. MMC knew of should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on MMC's systems.

141. MMC's own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. MMC's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. MMC's misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiffs' and Class Members' PII, including basic encryption techniques freely available to MMC.

142. Plaintiffs and Class Members had no ability to protect their PII that was in, and possibly remains in, MMC's possession.

143. MMC was in a superior and exclusive position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

144. MMC had and continues to have a duty to adequately and promptly disclose that the PII of Plaintiffs and Class Members within MMC's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

145. MMC had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and Class Members.

146. MMC has admitted that the PII of Plaintiffs and Class Members was wrongfully lost, disclosed to, and accessed by unauthorized third persons as a result of the Data Breach.

147. MMC, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and Class Members during the time the PII was within MMC's possession or control.

148. MMC further unlawfully breached its duties to Plaintiffs and the Class by failing to timely notify them of the breach, failing to disclose the precise PII impacted by the Data Breach, and failing to disclose other details that it did disclose in its Notice Letters to the Attorneys General and certain Class Members.

149. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation

PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

150. These foregoing frameworks are existing and applicable industry standards in the financial services industry, and Defendant failed to comply with these accepted standards thereby opening the door to the cyber incident and causing the data breach.

151. MMC improperly and inadequately safeguarded the PII of Plaintiffs and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

152. MMC failed to heed industry warnings and alerts to provide adequate safeguards to protect Students' PII in the face of increased risk of theft.

153. MMC, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Class Members' PII.

154. MMC, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and Class Members the existence and scope of the Data Breach.

155. But for MMC's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the PII of Plaintiffs and Class Members would not have been compromised.

156. There is a close causal connection between MMC's failure to implement security measures to protect the PII of Plaintiffs and Class Members and the harm suffered or risk of imminent harm suffered by Plaintiffs and the Class. Plaintiffs' and Class Members' PII was lost

and accessed as the proximate result of MMC's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

157. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as MMC, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of MMC's duty in this regard.

158. MMC violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. MMC's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and Class Members.

159. MMC's violation of Section 5 of the FTC Act demonstrates a prima facie case of negligence.

160. Plaintiffs and Class members are within the class of persons that the FTC Act was intended to protect.

161. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class.

162. As a direct and proximate result of MMC's negligence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and

recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in MMC's possession and is subject to further unauthorized disclosures so long as MMC fails to undertake appropriate and adequate measures to protect the PII in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (ix) the diminished value of MMC's goods and services they received.

163. As a direct and proximate result of MMC's negligence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

164. Additionally, as a direct and proximate result of MMC's negligence, Plaintiffs and Class members have suffered and will suffer the continued risks of exposure of their PII, which remains in MMC's possession and is subject to further unauthorized disclosures so long as MMC fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

COUNT II
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

165. Plaintiffs re-allege and incorporate by reference paragraphs above as if fully set forth herein.

166. Plaintiffs and Class Members conferred a monetary benefit on Defendant in the form of monetary payments—directly or indirectly—for providing education or employment to current and former students and employees.

167. Defendant collected, maintained, and stored the PII of Plaintiffs and Class Members and, as such, Defendant had knowledge of the monetary benefits it received on behalf of the Plaintiffs and Class Members.

168. The money that Plaintiffs and Class Members paid to Defendant should have been used to pay, at least in part, for the administrative costs and implementation of data security adequate to safeguard and protect the confidentiality of Plaintiffs' and Class Members' PII. Additionally, employees conferred a monetary benefit on Defendant as part of their salary and benefits was intended to apply to adequate data security which Defendant did not apply.

169. Defendant failed to implement—or adequately implement—those data security practices, procedures, and programs to secure sensitive PII, as evidenced by the Data Breach.

170. As a result of Defendant's failure to implement data security practices, procedures, and programs to secure sensitive PII, Plaintiffs and Class Members suffered actual damages in an amount of the savings and costs Defendant reasonably and contractually should have expended on data security measures to secure Plaintiff's PII.

171. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members because Defendant failed to implement the data security measures adequate to safeguard and protect the confidentiality of Plaintiffs' and Class Members' PII.

172. As a direct and proximate result of Defendant's decision to profit rather than provide adequate security, and Defendant's resultant disclosures of Plaintiffs' and Class Members'

PII, Plaintiffs and Class Members suffered and continue to suffer considerable injuries in the forms of time and expenses mitigating harms, diminished value of PII, loss of privacy, and a present increased risk of harm.

COUNT III
Breach of Express Contract
(On Behalf of Plaintiffs and the Class)

173. Plaintiffs re-allege and incorporate by reference the above paragraphs as if fully set forth herein.

174. This Count is plead in the alternative to Count II (Unjust Enrichment) above.

175. Plaintiffs and Class Members allege that they were the express, foreseeable, and intended beneficiaries of valid and enforceable express contracts between themselves and Defendant, contracts that (upon information and belief) include obligations to keep sensitive PII private and secure.

176. Upon information and belief, these contracts included promises made by Defendant that expressed and/or manifested intent that the contracts were made to primarily and directly benefit Plaintiffs and the Class, as Defendant's service was to provide education services in exchange for tuition payments from Plaintiffs and the Class, but also safeguarding the PII entrusted to Defendant in the process of providing these services, applying for those services, or applying for and/or accepting employment.

177. Upon information and belief, Defendant's representations required Defendant to implement the necessary security measures to protect Plaintiffs' and Class Members' PII. And to timely and accurately disclose the Data Breach to Plaintiffs and Class Members

178. Defendant materially breached its contractual obligation to protect the PII of Plaintiffs and Class Members when the information was accessed and exfiltrated by unauthorized personnel as part of the Data Breach.

179. Defendant materially breached its contractual obligations to Plaintiffs and the Class by failing to timely notify them of the breach, failing to disclose the precise PII impacted by the Data Breach, and failing to disclose the other details that it did disclose in its Notice Letters to the Attorneys General and certain Class Members.

180. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

181. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure of their PII, the loss of control of their PII, the present risk of suffering additional damages, and out-of-pocket expenses.

182. Plaintiffs and Class Members are entitled to compensator, consequential, and nominal damages suffered as a result of the Data Breach.

COUNT IV
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

183. Plaintiffs re-allege and incorporates by reference the foregoing paragraphs as if fully set forth herein.

184. This count is plead in the alternative to Count II (Unjust Enrichment) above.

185. Plaintiffs' and Class Members' PII was provided to Defendant as part of education services or employment that Defendant provided to Plaintiffs and Class Members.

186. Plaintiffs and Class Members agreed to pay Defendant tuition for education and administration services. Additionally, applicants for admission or employment agreed to provide their PII in exchange for Defendant's promise to keep it safe from unauthorized access.

187. Defendant and Plaintiffs and Class Members entered into implied contracts for the provision of adequate data security, separate and apart from any express contracts concerning the security of Plaintiffs' and Class Members' PII, whereby, Defendant was obligated to take reasonable steps to secure and safeguard Plaintiffs' and Class Members' PII.

188. Defendant had an implied duty of good faith to ensure that the PII of Plaintiffs and Class Members in its possession was only used in accordance with its contractual obligations.

189. Defendant was therefore required to act fairly, reasonably, and in good faith in carrying out its contractual obligations to protect the confidentiality of Plaintiffs' and Class Members' PII and to comply with industry standards and applicable laws and regulations for the security of this information.

190. Under these implied contracts for data security, Defendant was further obligated to provide Plaintiffs and all Class Members, with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII.

191. Defendant breached the implied contracts by failing to take adequate measures to protect the confidentiality of Plaintiffs' and Class Members' PII, resulting in the Data Breach.

192. Defendant further breached the implied contract by providing untimely notification to Plaintiffs and Class Members who may already be victims of identity fraud or theft or are at present risk of becoming victims of identity theft or fraud.

193. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

194. As a result of Defendant's conduct, Plaintiffs and Class Members did not receive the full benefit of the bargain.

195. Had Defendant disclosed that its data security was inadequate, neither Plaintiffs or Class Members, nor any reasonable person would have entered into such contracts with Defendant.

196. As a result of Data Breach, Plaintiffs and Class Members suffered actual damages resulting from the theft of their PII, as well as the loss of control of their PII, and remain at present risk of suffering additional damages.

197. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach, including the loss of the benefit of the bargain.

198. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, request judgment against the MMC and that the Court grant the following:

A. For an Order certifying the Class and appointing Plaintiffs and their Counsel to represent the certified Class;

B. For equitable relief enjoining MMC from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and the Class Members' PII, and from refusing to issue prompt, complete, any accurate disclosures to the Plaintiffs and the Class;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class, including but not limited to an order:

i. prohibiting MMC from engaging in the wrongful and unlawful acts described herein;

ii. requiring MMC to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring MMC to delete, destroy, and purge the personal identifying information of Plaintiffs and Class unless MMC can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and the Class;

iv. requiring MMC to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiffs' and Class Members' personal identifying information;

v. prohibiting MMC from maintaining Plaintiffs' and Class Members' personal identifying information on a cloud-based database;

vi. requiring MMC to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on MMC's systems on a periodic basis, and ordering MMC to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring MMC to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring MMC to audit, test, and train its security personnel regarding any new

or modified procedures;

ix. requiring MMC to segment data by, among other things, creating firewalls and access controls so that if one area of MMC's network is compromised, hackers cannot gain access to other portions of MMC's systems;

x. requiring MMC to conduct regular database scanning and securing checks;

xi. requiring MMC to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring MMC to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring MMC to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with MMC's policies, programs, and systems for protecting personal identifying information;

xiv. requiring MMC to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor MMC's information networks for threats, both internal and external, and assess

whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring MMC to meaningfully educate all class members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring MMC to implement logging and monitoring programs sufficient to track traffic to and from MMC's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate MMC's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of punitive damages;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: August 11, 2022

Respectfully Submitted,

s/ Blake Hunter Yagman

Blake Hunter Yagman
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC

100 Garden City Plaza, Suite 500
Garden City, New York 11530
Phone: (212) 594-5300
byagman@milberg.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
Fax: (865) 522-0049
gklinger@milberg.com

Terence R. Coates*
Justin C. Walker*
Jonathan T. Deters*
MARKOVITS, STOCK & DEMARCO, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
jwalker@msdlegal.com
jdeters@msdlegal.com

**pro hac vice forthcoming*

Attorneys for Plaintiffs and the Proposed Class